IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

U N I T E D S T A T E S	)	
	)	**DEFENSE REPLY TO**
v.	)	**GOVERNMENT RESPONSE TO**
	)	**DEFENSE MOTION TO DISMISS**
	)	**FOR FAILURE TO STATE AN**
MANNING, Bradley E., PFC	)	**OFFENSE: SPECIFICATIONS 13**
U.S. Army, (b) (6)	)	**AND 14 OF CHARGE II**
Headquarters and Headquarters Company, U.S.	)	
Army Garrison, Joint Base Myer-Henderson Hall,	)	DATED: 29 May 2012
Fort Myer, VA 22211	)	

RELIEF SOUGHT

1. PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 907(b)(1)(B), requests this Court to dismiss Specifications 13 and 14 of Charge II because the Government has failed to allege that PFC Manning's alleged conduct exceeded authorized access within the meaning of 18 U.S.C. Section 1030(a)(1).

ARGUMENT

2. At long last, the Government has clarified its theory of how PFC Manning allegedly exceeded his authorized access. The Government has specified that because PFC Manning's access to the SIPRNET computers was governed by a purpose-based limitation or restriction – namely, that he was "accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only" – he "exceeded authorized access when he accessed those classified government computers for an unauthorized or expressly forbidden purpose." Government Response to Defense Motion to Dismiss for Failure to State an Offense: Specifications 13 and 14 of Charge II [hereinafter Government Response], at 2. However, this purpose-based limitation or restriction theory of exceeds authorized access is, for the reasons articulated in the Defense Motion to Dismiss for Failure to State an Offense: Specifications 13 and 14 of Charge II [hereinafter Defense Motion],[1] premised on an impermissible interpretation of the phrase "exceeds authorized access," as that term is defined in 18 U.S.C. Section 1030(e)(6). The Government's arguments to the contrary are without merit.

3. The Defense agrees that the statutory text is clear and unambiguous. However, far from supporting the Government's expansive interpretation of the term "exceeds authorized access," the clear and unambiguous statutory definition of the term supports the Defense interpretation of the phrase: a person exceeds authorized access only when he accesses a computer with authorization and obtains or alters information on the computer that he is not entitled to obtain or

[1] All citations to the Defense Motion are to the page number, not to the numbered paragraph.

alter. Indeed, the Government has not cited any case finding that the clear and unambiguous meaning of the phrase supports the Government's expansive interpretation.

4. To the extent this Court concludes that the language of Section 1030(e)(6) is ambiguous, the legislative history of Section 1030(e)(6) and of Section 1030 as a whole supports the Defense's interpretation of "exceeds authorized access." The Government's assertion to the contrary is incorrect.

5. Moreover, the case law interpreting the phrase "exceeds authorized access" overwhelmingly supports the limited interpretation of that phrase advocated by the Defense. The cases relied on by the Government are poorly reasoned and incorrectly decided. The Government's attempt to distinguish this case from the many cases adopting the limited interpretation is entirely meritless.

6. Additionally, the Government is incorrect that the rule of lenity is inapplicable in this case. Even assuming, as the Government asserts, that application of the rule of lenity requires a "grievous ambiguity," that standard is clearly met here.

7. Finally, the Government fundamentally miscomprehends the Defense's discussion of vagueness. The Government erroneously focuses on PFC Manning's standing to assert a void-for-vagueness challenge when no such challenge was raised by the Defense Motion. The Government's misunderstanding must not distract this Court from addressing the Defense's actual argument that, as a matter of statutory construction, the fact that the Government's interpretation would render one provision of Section 1030 unconstitutionally vague provides yet another reason why the Government's interpretation should be rejected and the Defense's interpretation should be adopted.[2]

A. The Clear and Unambiguous Language of 18 U.S.C. Section 1030 Supports the Interpretation Advocated by the Defense

8. In its Response, the Government asserts that "the plain language of the statutory text clearly supports the Government's theory or interpretation of 'exceeds authorized access.'" Government Response, at 3. The Government does not cite a single case for this unequivocal assertion.

9. Additionally, the Government's desperate attempt to pin its interpretation on one word in the statutory definition – "so" – is without merit. That argument received full consideration by the en banc Ninth Circuit, at both oral argument and in its written opinion in *United States v. Nosal* (*Nosal III*), 676 F.3d 854 (9th Cir. 2012) (en banc), and was squarely rejected. The principal cases upon which the Government relies, *United States v. John*, 597 F.3d 263 (5th Cir. 2010), and *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), do not provide any support for the Government's heavy reliance on "so." In short, the only case to accept the Government's reliance on that one word was the panel majority in *United States v. Nosal* (*Nosal I*), 642 F.3d

[2] The Government offers no response to the Defense argument that overwhelming academic commentary supports the Defense's interpretation of the phrase "exceeds authorized access." Thus, the Government apparently does not dispute that, should this Court rule in favor of the Government on this issue, it would be ruling contrary to the established view of several computer crime scholars, including Professor Orin Kerr.

781 (9th Cir. 2011), and that decision was promptly rejected by the en banc Ninth Circuit in *Nosal III*. Moreover, the Defense's interpretation of the phrase "exceeds authorized access" does not, as the Government asserts, read the word "so" out of the statute. Rather, it is the Government's interpretation that requires the Court to rewrite the clear and unambiguous text of Section 1030(e)(6) by unjustifiably ascribing an expansive meaning to the simple word "so."

10. Finally, the Government simply ignores the Defense argument that the language of the specifications in this case further demonstrate that the language of Section 1030(e)(6) is clear and unambiguous. The Government's inability to effectively respond to this argument is yet additional evidence that the Government's argument regarding the clear and unambiguous language is meritless.

11. Therefore, this Court should determine that the clear and unambiguous language of Section 1030(e)(6) supports the Defense's proposed interpretation of the phrase "exceeds authorized access."

12. As an initial matter, the Government does not cite a single case for its assertion that the clear and unambiguous language of Section 1030(e)(6)'s definition of the phrase "exceeds authorized access" supports its interpretation. *John* and *Rodriguez*, the two cases upon which the Government principally relies, offer no such support, as neither case referred to Section 1030 as "clear" or "unambiguous." The Government's lack of citation speaks volumes about the weakness of its position. In its Motion, the Defense cited numerous cases supporting its contention that the clear and unambiguous language of Section 1030(e)(6) mandates the more limited interpretation of "exceeds authorized access:" a person exceeds authorized access only when he accesses a computer with authorization and obtains or alters information on the computer that he is not entitled to obtain or alter. *See, e.g., United States v. Zhang*, No. CR-05-00812 RMW, 2010 WL 4807098, at *3 (N.D. Cal. Nov. 19, 2010) ("Nonetheless, a plain reading of [S]ection 1030(e)(6)'s definition . . . compels a different conclusion. An individual 'exceeds authorized access' if he or she has permission to access a portion of the computer system but uses that access to 'obtain or alter information in the computer that [he or she] is not entitled so to obtain or alter.' As the court in *Norsal* [sic] explained, 'there is simply no way to read that definition to incorporate policies governing use of information unless the word alter is interpreted to mean misappropriate.'" (citations omitted)); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 (S.D.N.Y. 2010) ("The Government's theory that the CFAA is violated whenever an individual uses information on a computer in a manner contrary to the information owner's interest would therefore require a departure from the plain meaning of the statutory text."); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The plain language of [Section 1030] supports a narrow reading. [Section 1030] expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation."); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) ("[T]he plain language of [Section] 1030(a)(2), (4), and (5)(A)(iii) target 'the unauthorized procurement or alteration of information, not its misuse or misappropriation.'"). In response, the Government asks this Court to hold that the clear and unambiguous meaning of Section 1030(e)(6) supports the expansive interpretation of the phrase, and it offers this Court no authority to support such an unwarranted step.

13. Even more troubling is the Government's "so" argument.[3] The Government explains that, in its view, "so" has the following meaning: "'So' means '[i]n the state or manner indicated or expressed.' According to the Government, the presence of 'so' after 'entitled' in § 1030(e)(6) makes the definition unambiguous – an individual 'exceeds authorized access' when he or she obtains or alters information that he or she is not entitled to obtain or alter *in those circumstances*." Government Response, at 4 (citation omitted) (emphasis and alteration in original).

14. This interpretation of "so" was roundly rejected by the en banc Ninth Circuit in *Nosal III*. *See* 676 F.3d at 857-58. In the *Nosal III* oral argument in December 2011, the government argued that the use of the word "so" was critically important in the drafting and interpretation of the statute. Indeed, the government seemed to suggest that the entire interpretation of Section 1030 hinged on this two-letter word. The judges did not appear impressed with the government's argument, and they harped on what they saw as the government's strained interpretation of the word "so." At various points early in the argument, the judges expressed their concern:

> I guess I'm not sure why that [interpretation of 'so'] is necessary . . . it's possible. Why can't you read the 'so' as applying to physical restrictions?
>
> . . .
>
> But that's not necessarily the case . . . where actually you do have physical access, you can do it but you're just not allowed to go there. You're not required to do any hacking, it's simply they say you are not authorized to go into that area. Why isn't that [interpretation of 'so'] possible?
>
> . . .

[3] The Government's argument in this respect is essentially a cut-and-paste of the panel majority's decision in *Nosal I*:

> The government contends that Nosal's interpretation of "exceeds authorized access" would render superfluous the word "so" in the statutory definition. We agree. "So" in this context means "in a manner or way that is indicated or suggested." *Webster's Third New Int'l Dictionary* 2159 (Philip Babcock Gove, ed.2002). Thus, an employee exceeds authorized access under § 1030(e)(6) when the employee uses that authorized access "to obtain or alter information in the computer that the accesser is not entitled [in that manner] to obtain or alter." We decline to render meaningless a word duly enacted by Congress. *See Corley v. United States*, 556 U.S. 303, 129 S.Ct. 1558, 1566, 173 L.Ed.2d 443 (2009) ("[O]ne of the most basic interpretive canons [is] that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." (internal quotation marks and alteration omitted)). Because the statute refers to an accesser who is not entitled to access information in a certain manner, whether someone has exceeded authorized access must be defined by those access limitations. The plain language of the statute supports the government's interpretation."

Nosal I, 642 F.3d at 785-86. This argument was emphatically rejected by the overwhelming majority of the en banc Ninth Circuit in *Nosal III*. *See* 676 F.3d at 857-58.

> But if you're not permitted . . . and you do it anyway . . . you're not allowed to go there. And if you do, you're violating . . . the restrictions in which case, you are doing it . . . . I don't know why that isn't just . . . . I don't know why that doesn't give effect to the word 'so' just as you would if you were accessing it with an improper motive.
>
> . . .
>
> But that's not the question. The question is not whether you could do better job of drafting, the question is whether this is a necessary meaning [of 'so'] . . . . Now the fact that it could have been better drafted . . . I go back and read some of my opinions from 20 years ago and I have a bunch of words I wished I'd left out. Every time you go back and redraft something you say, "oh god what was I thinking of." But unless it's necessary [to interpret 'so' as you suggest], then it seems to me that the answer you have to give is "That's a possible interpretation." Once we're in the world of possible interpretation, aren't we then required by the rule of lenity to adopt the one that sweeps in the least number of people?

Oral Argument at 5:29, 6:24, 7:46, 8:41, United States v. Nosal, 676 F.3d 854 (No. 10-10038), *available at* http://www.ca9.uscourts.gov/media/view_video_subpage.php?pk_vid=0000006176. This skepticism fermented into outright rejection in the en banc majority opinion:

> The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. This places a great deal of weight on a two-letter word that is essentially a conjunction. If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions – which may well include everyone who uses a computer – we would expect it to use language better suited to that purpose.

676 F.3d at 857.

15. Moreover, *John* and *Rodriguez* do not support the Government's heavy reliance on "so." For one thing, neither case gave any indication that the word "so" was critical to the holding. For another thing, at least one of these courts – the *Rodriguez* Court – mistakenly omitted the word "so" from its quotation of Section 1030(e)(6): "The Act defines the phrase 'exceeds authorized access' as 'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter.'" 628 F.3d at 1263 (quoting 18 U.S.C. § 1030(e)(6)) (mistakenly omitting word "so" between "entitled" and "to"); *see* 18 U.S.C. § 1030(e)(6). Thus, not only did both of the appellate cases upon which the Government principally relies not place any emphasis whatsoever on the word "so," one of those cases actually omitted this supposedly critical word from its quotation of the statutory definition. This provides further support for the conclusion that the Government's desperate reliance on "so" is untenable.

16. Of the cases cited by the Government, only the Ninth Circuit panel majority in *Nosal I* bought the Government's "so" argument. *See* 642 F.3d at 785-86. That decision was promptly rejected by an overwhelming majority of the en banc *Nosal III* Court. *See* 676 F.3d at 857. What the Government's argument in this case comes down to, then, is a plea for this Court to ignore the recent, directly on point decision of an en banc United States Court of Appeals and strike out on its own, resurrecting a meritless argument that the *Nosal III* Court has persuasively laid to rest. This Court should reject this hopeless plea.

17. Additionally, contrary to the Government's assertion, the interpretation of "exceeds authorized access" offered by the Defense does not render the word "so" superfluous. In its Response, the Government asserts that "[a]lthough the defense does not address the issue, the only conclusion that can be reached is that they consider the word 'so' to be superfluous." Government Response, at 4. Even a cursory reading of the Defense Motion reveals that this statement is flatly incorrect in both respects; the Defense did address the issue, and the Defense offered an interpretation of the phrase "exceeds authorized access" that did not render "so" superfluous. The Defense continues to assert, as it did in the Defense Motion, that "Congress could just as well have included 'so' as a connector or for emphasis." *Nosal III*, 676 F.3d at 858; *see* Defense Motion, at 13 (quoting this language). This interpretation of "exceeds authorized access" does not render "so" superfluous, and it has the added benefit, conspicuously absent from the Government's interpretation, of not relying on a two-letter word to "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Nosal III*, 676 F.3d at 857.

18. Indeed, it is the Government's interpretation of "so," not the Defense's interpretation, that requires this Court to rewrite the clear and unambiguous language of Section 1030(e)(6). By the Government's own admission, for the Government to "prevail" this Court would need to interpret Section 1030(e)(6) to read "an individual 'exceeds authorized access' when he or she obtains or alters information that he or she is not entitled to obtain or alter *in those circumstances*." Government Response, at 4 (emphasis in original). This Court should follow the wise lead of other courts and reject the request that it pick up a legislator's pen to rewrite this statute. *See, e.g.*, *Walsh Bishop Assocs., Inc. v. O'Brien*, No. 11-2673 (DSD/AJB), 2012 WL 669069, at *3 (D. Minn. Feb. 28, 2012) ("The language of [Section] 1030(a)(2) does not support the interpretation of Walsh Bishop. Instead, Walsh Bishop's interpretation requires the court to rewrite the statute to replace the phrase 'to use such access to obtain or alter information that the accesser is not entitled so to obtain or alter' with 'to use such information in a manner that the accesser is not entitled so to use.' But subsection (a)(2) is not based on use of information; it concerns access. Indeed, the language of subsection (a)(1) shows that Congress knows how to target the use of information when it intends to do so."). Therefore, the Government's "so" argument should be rejected.

19. In addition to the lack of case law in support of the Government's "clear and unambiguous" argument and its meritless "so" argument, the Government's contention that the clear and unambiguous language of Section 1030 supports its interpretation of the term "exceeds authorized access" is flawed for another reason: it fails to address the Defense's argument that the specifications in this case demonstrate that Section 1030's clear and unambiguous text favors the limited interpretation advocated by the Defense. In the Section 1030(a)(1) specifications, the

Government alleges, in pertinent part, that PFC Manning "knowingly *exceeded authorized access* on a Secret Internet Protocol Router Network computer, *and by means of such conduct having obtained information* . . . ." Charge Sheet, Specification 13 (emphases supplied). It is clear from this specification that "exceeding authorized access" is different from, and a predicate to, "obtaining information."

20. However, if the term "exceeded authorized access" is interpreted as the Government suggests, the charge would be redundant and nonsensical. It would allege, in pertinent part, that PFC Manning "knowingly ["accessed that computer . . . to obtain these documents," *see* Oral Argument, Unauthenticated Transcript, 23 February 2012, pp. 71-72] on a Secret Internet Protocol Router Network computer, and by means of such conduct having obtained information . . . ." Charge Sheet, Specification 13 (alteration supplied). Thus read, the charge does not make sense since "exceeding authorized access" is conflated with obtaining documents for an improper purpose, which is the next part of the specification ("by means of such conduct having obtained information"). Thus, the exceeding authorized access cannot be the same as "obtain[ing] information" or the specification falls apart. This provides further evidence that the plain meaning of the statute is clear: Section 1030 asks only whether the accused had authorized access to the computer and information in question. It does not contemplate an inquiry into what an accused otherwise does with properly accessed information. The Government's inability to effectively respond to this argument is yet additional evidence that the Government's argument regarding the clear and unambiguous language is meritless.

21. In the end, Section 1030(a)(1) prohibits "exceeding authorized access," not "exceeding authorized use." The Government's interpretation, in conflating the concepts of "access" and "use," impermissibly attempts to punish PFC Manning for exceeding his authorized use. This cannot be done. *See Lewis-Burke Assocs. LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010) ("'Exceeds authorized access' should not be confused with exceeds authorized use." (internal quotations omitted)); *Bell Aerospace Servs, Inc. v. U.S. Aero Services, Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010) ("'Exceeds authorized access' should not be confused with exceeds authorized use.").

22. For these reasons and those stated in the Defense Motion, the clear and unambiguous language of the definition of "exceeds authorized access" supports the limited interpretation of that phrase: a person exceeds authorized access only when he accesses a computer with authorization and obtains or alters information on the computer that he is not entitled to obtain or alter.

B. The Legislative History of 18 U.S.C. Section 1030 Supports the Interpretation Advocated by the Defense

23. To the extent this Court determines that the Government's proposed interpretation of the phrase "exceeds authorized access" is a plausible one, and thus concludes that the language of Section 1030(e)(6) is ambiguous, the legislative history of Section 1030(e)(6) and of Section 1030 as a whole supports the Defense's interpretation of "exceeds authorized access." The Government is incorrect that the 1986 Amendments to Section 1030 support its interpretation;

indeed, it does not cite even one case stating that the legislative history lends itself to an expansive reading of "exceeds authorized access." By contrast, many of the cases cited by the Defense have concluded that the legislative history supports a limited interpretation of "exceeds authorized access" and have rejected the expansive interpretation advocated by the Government.

24. The Ninth Circuit in *Nosal III*, for example, explained that Congress's replacement of the phrase "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" with the phrase "exceeds authorized access" supported the limited interpretation of that phrase that it adopted, and further undermined the Government's proposed interpretation. 676 F.3d at 858 n.5. Along similar lines, the *Alyenikov* Court explained:

> Notably, in 1986, Congress amended the CFAA to substitute the phrase "exceeds authorized access" for the phrase "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." *See* S.Rep. No. 99–432, at 9, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2486. By enacting this amendment, and providing an express definition for "exceeds authorized access," Congress's intent was to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,'" thereby "remov[ing] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization." *Id.* at 21, 1986 U.S.C.C.A.N. at 2494–95.

737 F. Supp. 2d at 192 n.23. Several other courts have echoed similar sentiments. *See, e.g.*, *Walsh Bishop Assocs., Inc.*, 2012 WL 669069, at *3 ("Further, the legislative purpose and history supports the plain meaning of the statute. Congress enacted [Section 1030] to deter 'the criminal element from abusing computer technology in future frauds.' H.R. Rep. No. 98–894, at 4 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3690. As originally enacted, [Section 1030] applied to a person who (1) knowingly accessed without authorization or (2) 'having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.' Pub. L. No. 98–473, § 2102, 98 Stat. 2190, 2190–91 (1984). Congress amended the statute by replacing the latter means of access with the phrase 'exceeds authorized access.' *See* Pub. L. No. 99–474, § 2, 100 Stat. 1213, 1213 (1986). The stated reason for the amendment was to 'eliminate coverage for authorized access that aims at purposes to which such authorization does not extend.' *See* S. Rep. No. 99–432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2495 (internal quotation marks omitted). As a result, Congress amended the statute to remove use as a basis for exceeding authorization."); *Condux Int'l, Inc. v. Haugum*, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *5 (D. Minn. Dec. 15, 2008) ("Had Congress [under Section 1030] intended to target how a person makes use of information, it would have explicitly provided language to that effect."); *Shamrock Foods*, 535 F. Supp. 2d at 966 ("[T]he legislative history confirms that [Section 1030] was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (explaining the purpose of the change in legislative language).

25. Thus, the Government's interpretation of the legislative history has been soundly rejected by both appellate and trial courts, in both the civil and criminal context. It should be likewise rejected by this Court.

26. Accordingly, for these reasons and those stated in the Defense Motion, the legislative history of Section 1030 provides further support for the interpretation of "exceeds authorized access" advocated by the Defense and further undermines the interpretation advocated by the Government.

C. Case Law Supports the Interpretation Advocated by the Defense

27. The case law interpreting the phrase "exceeds authorized access" overwhelmingly supports the limited interpretation of that phrase advanced by the Defense. The cases relied on by the Government are poorly reasoned and, not surprisingly, incorrectly decided. Moreover, the Government's vain attempt to distinguish this case from the litany of cases adopting the limited interpretation is entirely without merit. *John* and *Rodriguez*, upon which the Government places principal reliance, are emblematic of the flawed reasoning that adopts the expansive interpretation of "exceeds authorized access." Neither the *John* Court nor the *Rodriguez* Court offered any explanation – much less any plausible explanation – as to how its interpretation of "exceeds authorized access" could be squared with the plain meaning of Section 1030. As the court stated in *Aleynikov*:

> [These cases] identify no statutory language that supports interpreting [Section 1030] to reach misuse or misappropriation of information that is lawfully accessed. Instead, they improperly infer that "authorization" is automatically terminated where an individual "exceed[s] *the purposes* for which access is 'authorized.'" But "the definition of 'exceeds authorized access' in [Section] 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word 'authorization.'"

737 F. Supp. 2d at 193 (emphasis supplied) (citations omitted).

28. The en banc *Nosal* Court further pointed out that the *Rodriguez* and *John* decisions were the product of the courts' failure to consider the broader implications of their holdings. The *Nosal III* Court explained that:

> These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access." They therefore failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid "making criminal law in Congress's stead."

676 F.3d at 862-63 (quoting *United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality opinion)). In short, the Defense has used far more ink in criticizing *John* and *Rodriguez* than

those courts used in their "analysis" of the phrase "exceeds authorized access." The perfunctory discussion and short-sighted reasoning employed by the *John* and *Rodriguez* Courts should leave any court highly skeptical of the Government's expansive interpretation.

29. The only other two criminal cases identified by the Government – *United States v. Salum*, 257 F. App'x 225 (11th Cir. 2007) and *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997) – are even worse. These cases offer no analysis and simply state in conclusory fashion that the defendant exceeded his authorized access.

30. Understandably concerned with the dearth of quality case law supporting its position, the Government attempts to distinguish this case from the multiple authorities supporting the Defense's position. The Government asserts that the cases cited by the Defense, other than *Nosal III*, "did not consider . . . explicit purpose-based restrictions or limitations on computer access." Government Response, at 8. This argument is meritless.

31. To the extent the Government is attempting to draw a distinction between "explicit purpose-based restrictions or limitations" and implicit purpose-based restrictions or limitations – and it is not at all clear what the Government means when it says "explicit" – such a distinction finds no support in Section 1030, its legislative history, or the case law interpreting it. The expansive interpretation defines exceeding authorized access in terms of the purposes for which the computer is accessed or the purposes for which the information is obtained. Under this theory, the purpose for which the computer is accessed or the information is obtained controls whether access has been exceeded. In the typical case, a defendant uses a computer to obtain information for non-business purposes, and defendant thereby exceeds authorized access. There is no basis in law or logic for distinguishing cases where there is a contractual or other "explicit" restriction on computer use for non-business purposes from cases where there is some type of agency-based restriction on computer use for non-business purposes. In either type of case, the purpose of the user in accessing the computer or obtaining the information controls whether the user has "exceeded authorized access."

32. In any event, the Government is simply wrong that the cases cited by the Defense do not involve explicit purpose-based restrictions. A simple examination of each of the cases "distinguished" by the Government reveals that each involved an explicit purpose-based restriction on the defendant's use of the computer or the information. *See Walsh Bishop Assocs., Inc.*, 2012 WL 669069, at *4 n.4 (explicit purpose-based restriction: "the [computer-use] policy defines inappropriate use as: 'Revealing or publicizing proprietary, confidential or private information . . . Sending (upload) or receiving (download) copyrighted materials, trade secrets, proprietary information or similar materials without prior authorization . . . making unauthorized use of the intellectual property or proprietary data of ours or others.'"); *Xcedex, Inc., v. VMware, Inc.*, No. 10-3589 (PJS/JJK), 2011 WL 2600688, at *4 (D. Minn. June 8, 2011) (explicit contractual purpose-based restriction: "According to the Amended Complaint, the 2009 Work Order 'confirmed that Xcedex [plaintiff] would deliver authorization to access and use its X_Factor software as a service' but limited such access and use to '4,000 devices and licenses.'"); *Aleynikov*, 737 F. Supp. 2d at 175 (explicit contractual purpose-based restriction: "Goldman [the employer] also limits access to the Trading System's source code only to Goldman employees who have reason to access that source code, such as the programmers

working on the Trading System."); *Int'l Ass'n of Machinists & Aerospace Workers*, 390 F. Supp. 2d 479, 498 (explicit contractual purpose-based restriction: "Defendant Werner-Matsuda signed a Registration Agreement stipulating not to use the information provided through VL lodge for any purpose that would be contrary to the policies and procedures established by the [IAM] Constitution."). The same can be said for the other cases cited in the Defense motion. In short, the purpose-based restrictions in the cases cited in the Defense Motion are no different in kind from the purpose-based restriction that the Government contends existed in this case.

33. More importantly, the Government's confusion on this point should not draw attention away from the ultimate inquiry. Any type of purpose-based restriction, whether explicit or implicit, focuses on the defendant's *use* of the computer or information (e.g. is the defendant using the computer or obtaining the information for non-business purposes?). Section 1030(e)(6), however, makes clear that the inquiry should be directed to the user's *access* to that computer and information (e.g. is the user accessing information to which his authorization does not extend?). *See Lewis-Burke Assocs. LLC*, 725 F. Supp. 2d at 194 ("'Exceeds authorized access' should not be confused with exceeds authorized use." (internal quotations omitted)); *Bell Aerospace Servs, Inc.*, 690 F. Supp. 2d at 1272 ("'Exceeds authorized access' should not be confused with exceeds authorized use."). Therefore, any purpose-based restriction theory should be rejected as untenable.

34. Accordingly, for these reasons and those stated in the Defense Motion, the overwhelming majority of the persuasive case law on the interpretation of the phrase "exceeds authorized access" supports the interpretation advanced by the Defense: a person exceeds authorized access only when he accesses a computer with authorization and obtains or alters information on the computer that he is not entitled to obtain or alter.

D. The Rule of Lenity Requires That "Exceeds Authorized Access" Be Read in Its Narrow Sense

35. The Defense continues to maintain that the clear and unambiguous language of Section 1030 supports the limited interpretation of "exceeds authorized access." Only if this Court determines that the Government's expansive interpretation is plausible, and that Section 1030 is therefore ambiguous, must this Court consider the rule of lenity. If this Court does determine that Section 1030's definition of "exceeding authorized access" is ambiguous, the rule of lenity is one of the many factors that, along with Section 1030's legislative history, well-established principles of statutory construction, case law interpreting the phrase "exceeding authorized access" and the academic commentary on Section 1030, supports the conclusion that the Defense's limited interpretation is more appropriate than the Government's. The Government's formulaic invocation of a "grievous ambiguity" standard, with no analysis of the ambiguity that would be present in this case if both the limited and expansive interpretations of "exceeding authorized access" are permissible, provides the Government with no relief. The ambiguity that results if both the Defense's and the Government's interpretations are plausible is surely grievous enough to warrant application of the rule of lenity.

36. At the outset, it should be noted that the Government has cited no case from a military court that applies the "grievous ambiguity" standard for the rule of lenity. *See* Government Response, at 8-9. The Defense's research revealed no military decision even using the words "grievous" and "ambiguity," or some variant of those terms, in the same sentence. Moreover, a careful look at Supreme Court precedent suggests that the Court does not actually use a "grievous" ambiguity standard and that the expression is only referred to in passing.[4] Nonetheless, even assuming, *arguendo*, that the "grievous ambiguity" standard articulated in the Government's Response is the controlling standard for the rule of lenity, the rule of lenity should still be applied in this case if the Court determines that both interpretations of "exceeds authorized access" are plausible.

37. Under *Barber v. Thomas*, 130 S. Ct. 2499 (2010) and *Muscarello v. United States*, 524 U.S. 125 (1998), the two cases cited by the Government for the "grievous ambiguity" standard, *see* Government Response, at 8-9, a "grievous ambiguity" exists where "the Court must simply guess as to what Congress intended." *Barber*, 130 S. Ct. at 2508-09 (internal quotations omitted); *see Muscarello*, 524 U.S. at 138-39.

38. In its Response, the Government has simply mouthed this standard and asserted, in conclusory fashion, that no grievous ambiguity exists. *See* Government Response, at 8-9. Upon closer inspection, however, it becomes clear that if this Court concludes that both interpretations of "exceeds authorized access" that have been advanced by the parties are permissible, Section 1030 does contain the requisite "grievous ambiguity."

39. The Supreme Court's decision in *Muscarello* provides an apt example of why this is so. In *Muscarello*, the issue was "whether the phrase 'carries a firearm' [used in 18 U.S.C. Section 924(c)] is limited to the carrying of firearms on the person." 524 U.S. at 126. In resolving this issue, the Court concluded that the term "carry" had an ordinary meaning and that Congress intended for that ordinary meaning to govern the phrase "carries a firearm." *Id.* at 127-131. This ordinary meaning supported the Government's interpretation and undermined the defendants' interpretation. *See id.* Additionally, the Court noted that the question had not perplexed the courts of appeals; instead, those courts were in unanimous agreement that the ordinary meaning of the term "carry" applied to Section 924(c). *Id.* at 131-32. These factors led the Court to conclude that its decision was "based on much more than a 'guess as to what Congress intended,' and [that] there [was] no 'grievous ambiguity[.]'" *Id.* at 139.

40. This case, by contrast, possesses none of the factors identified by the Court in *Muscarello*. For one thing, to the extent there is a commonly understood, ordinary meaning of "exceeds authorized access" the Defense submits that it favors the limited interpretation. Certainly the Government cannot claim that its expansive interpretation, which conflates the concepts of "access" and "use," *see* Argument, Part A, *supra*, is supported by any commonly understood, ordinary meaning of "exceeds authorized *access*," if such an ordinary meaning exists. Thus,

[4] In a search of Supreme Court case law, there were 7 cases that referred to "grievous ambiguity" in reference to the rule of lenity. Most of these 7 cases simply cross-referenced each other. By contrast, there were 72 Supreme Court cases that did not use the grievous ambiguity standard when applying the rule of lenity. These cases articulated the doctrine as some variation of the following: "The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them." *See United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality opinion). Moreover, as discussed, military courts have not adopted a "grievous ambiguity" standard.

unlike in *Muscarello*, the Government's interpretation is not supported by the ordinary meaning of the phrase under examination. Also, far from being uniform on this issue, most courts of appeals have not addressed the issue of the proper interpretation of the phrase "exceeds authorized access" under Section 1030. The few that have examined the issue have come to widely divergent results. *Compare Nosal III*, 676 F.3d at 863-64 (adopting limited interpretation), *with John*, 597 F.3d 263 (adopting expansive interpretation), *and Rodriguez*, 628 F.3d 1258 (same); *see also Ajuba Intern., L.L.C. v. Saharia*, No. 11-12936, 2012 WL 1672713, at *10 (E.D. Mich. May 14, 2012) ("The parties' dispute reflects a nationwide split of authority concerning the proper interpretation of the terms 'without authorization' and 'exceeds authorized access.'). Therefore, if both the expansive interpretation and the limited interpretation of "exceeds authorized access" are permissible then, with a circuit split and no ordinary meaning supporting the Government's interpretation, courts are left to simply venture a guess as to what Congress intended the phrase to mean. Thus, the requisite "grievous ambiguity" exists.

41. Moreover, the difference between the conduct that is punishable under the two interpretations of "exceeding authorized access" is hardly academic. As discussed elsewhere, *see* Defense Motion, at 21-24; *see also* Argument Part E, *infra*, a staggering amount of conduct is punishable under the expansive interpretation that would not be punishable under the limited interpretation. This wide gulf between the conduct that is punishable under the varying interpretations is even further evidence of the "grievous ambiguity" that exists.

42. Indeed, this was precisely the concern that led the *Nosal III* Court to rely, at least in part, on the rule of lenity in reaching its conclusion. The *Nosal III* Court explained that, given the wide range of conduct made punishable under the Government's interpretation of "exceeds authorized access," the rule of lenity should be invoked:

> In *United States v. Kozminski*, 487 U.S. 931, 108 S.Ct. 2751, 101 L.Ed.2d 788 (1988), the Supreme Court refused to adopt the government's broad interpretation of a statute because it would "criminalize a broad range of day-to-day activity." *Id.* at 949, 108 S.Ct. 2751. Applying the rule of lenity, the Court warned that the broader statutory interpretation would "delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes" and would "subject individuals to the risk of arbitrary or discriminatory prosecution and conviction." *Id.* By giving that much power to prosecutors, we're inviting discriminatory and arbitrary enforcement.
>
> We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty. *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir.2010); *United States v. John*, 597 F.3d 263 (5th Cir.2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir.2006). These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access." They therefore failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to

> avoid "making criminal law in Congress's stead." *United States v. Santos*, 553 U.S. 507, 514, 128 S.Ct. 2020, 170 L.Ed.2d 912 (2008).

676 F.3d at 862-63.

43. Therefore, for these reasons and those articulated in the Defense Motion, this Court should, if it determines that Section 1030(e)(6) is ambiguous, apply the rule of lenity and adopt the limited interpretation of "exceeds authorized access" advocated by the Defense.

E. The Government Profoundly Misunderstands the Defense's Vagueness Discussion

44. Of all the meritless arguments made in the Government's Response, the most glaring is the Government's response to the Defense's vagueness discussion. Whether it honestly misunderstood the Defense's argument or attempted to use its void-for-vagueness response as a red herring, the Government mistakenly focuses on PFC Manning's standing to make a void-for-vagueness claim. In so doing, the Government offers no response to the Defense's real argument concerning the vagueness of one provision of Section 1030: because the interpretation of "exceeds authorized access" chosen by a court applies to *all* provisions of Section 1030 in which that phrase is used and because the Government's expansive interpretation would render one of those provisions unconstitutionally vague, *as a matter of statutory construction*, this Court must adopt the narrower interpretation to save Section 1030's constitutionality.

45. In the event that the Defense Motion was at all unclear on this point, the Defense now reiterates that the vagueness section of its Motion, *see* Defense Motion, at 21-24, was *not* making a void-for-vagueness challenge to Section 1030(a)(1), or any other subsection of Section 1030, on PFC Manning's behalf. Rather, the Defense was merely illustrating the vagueness problems that the Government's interpretation would pose for one provision of Section 1030. And since the interpretation of "exceeds authorized access" chosen by a court in *any* Section 1030 prosecution must apply to *all* provisions of Section 1030 using that phrase, the Court must, as a matter of statutory construction, consider the vagueness issues the Government's interpretation poses in selecting the proper interpretation of the phrase. When the Defense's argument is viewed in this appropriate light, the Government's discussion of which provisions of Section 1030 PFC Manning does and does not have standing to challenge on vagueness grounds is nonresponsive to the Defense's argument and entirely beside the point.

46. In the course of discussing PFC Manning's standing to raise a vagueness challenge, the Government asserts the following: "An interpretation of a phrase under § 1030(a)(1) that may lead to absurd results under another provision of § 1030 is irrelevant to the issues before this Court." Government Response, at 9. This statement could not be further from the truth.

47. It is a bedrock principle of statutory construction that "identical words and phrases within the same statute should normally be given the same meaning." *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007); *see Nosal III*, 676 F.3d at 859 (quoting this language). This principle makes manifest that the interpretation given to "exceeds authorized access" under any provision of Section 1030 must also be given to all other provisions of Section 1030 where

this phrase appears. *See Nosal III*, 676 F.3d at 859. Additionally, the Government has helpfully cited *Corley v. United States*, 556 U.S. 303 (2009), a case which supports the Defense's position. In *Corley*, the Court discussed "one of the most basic interpretative canons, that '[a] statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, *void* or insignificant.'" 556 U.S. at 314 (quoting *Hibbs v. Winn*, 542 U.S. 88, 101 (2004)) (emphasis supplied). In *Corley*, the Court found that "[t]he fundamental problem with the Government's reading of [the subsection at issue] is that it renders [another subsection] nonsensical and superfluous." *Id.* at 314. Thus, *Corley* recognizes that an interpretation of a certain provision of a statute must be reconciled with what that interpretation would mean for another section of that same statute.

48. Taken together, the principles of statutory construction identified in *Powerex Corp.* and *Corley* readily demonstrate why the Government's above-quoted assertion that is utterly baseless and flatly incorrect: where, as here, a statute uses identical words and phrases within a statute (such that those identical words and phrases must be given the same meaning), a court may not construe a provision in that statute in a way that renders any provision of it void. *See Corley*, 556 U.S. at 314; *Powerex Corp.*, 551 U.S. at 232. The Government's suggestion that "[a]n interpretation of a phrase under § 1030(a)(1) that may lead to absurd results under another provision of § 1030 is irrelevant to the issues before this Court[,]" Government Response, at 9, completely ignores these fundamental principles.

49. Remarkably, the Government's statement perfectly mirrors the discredited argument of the government in *Nosal III*:

> The government argues that our ruling today would construe "exceeds authorized access" only in subsection 1030(a)(4), and we could give the phrase a narrower meaning when we construe other subsections. This is just not so: Once we define the phrase for the purpose of subsection 1030(a)(4), that definition must apply equally to the rest of the statute pursuant to the "standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning." *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232, 127 S.Ct. 2411, 168 L.Ed.2d 112 (2007). The phrase appears five times in the first seven subsections of the statute, including subsection 1030(a)(2)(C). *See* 18 U.S.C. § 1030(a)(1), (2), (4) and (7). Giving a different interpretation to each is impossible because Congress provided a *single* definition of "exceeds authorized access" for all iterations of the statutory phrase. *See id.* § 1030(e)(6). Congress obviously meant "exceeds authorized access" to have the same meaning throughout [S]ection 1030. We must therefore consider how the interpretation we adopt will operate wherever in that section the phrase appears.

676 F.3d at 859 (emphasis in original). This point was also clearly stated in the Defense Motion. *See* Defense Motion, at 22-23 n.12.

50. At bottom, the Government is, through a misplaced focus on PFC Manning's standing to raise a *vagueness challenge*, inviting this Court to ignore well-established principles of *statutory*

construction in determining which interpretation of the phrase "exceeds authorized access" to adopt. This Court should, based on the principles of *Corley* and *Powerex Corp.* and for the reasons stated in *Nosal III*, decline that invitation.

51. Therefore, the fact that a particular interpretation of "exceeds authorized access" could render another provision of Section 1030 unconstitutionally vague is indeed relevant to this Court's inquiry into the proper interpretation of that phrase. In the Defense Motion, the Defense identified several reasons why the expansive interpretation of "exceeds authorized access" would render Section 1030(a)(2)(C) unconstitutionally vague. The Government has offered no rebuttal to this argument; it instead focused on what it erroneously perceived as an obstacle to the Court's consideration of the arguments (i.e. PFC Manning's standing to raise a vagueness challenge). The Defense will therefore not repeat the many unopposed arguments as to why the expansive interpretation of "exceeds authorized access" renders Section 1030(a)(2)(C) unconstitutionally vague.

52. However, now that the Government has finally specified its theory of "exceeds authorized access" – namely, that the warning banner on a Government computer stating that the computer is to be used for Government-authorized use only constitutes an explicit purpose-based restriction on access, *see* Government Response, at 1-2 – a brief comment on the vagueness concerns for users of Government computers is warranted. This theory clearly implicates the constitutional vagueness concerns specified in the Defense Motion. Warning banners like the one referenced by the Government in its Response, *see id.*, are commonplace for Government computers. If a Soldier lawfully accesses a Government computer displaying a warning banner of this type, but then checks his or her personal email, or sports scores, or any of the other countless trivial things people do on their computers in a day's work, the Soldier will have committed a federal offense under Section 1030(a)(2)(C) if the Government's interpretation is accepted. How can a Soldier be expected to know that his occasional innocent use of his computer for some trivial personal purpose could lead to his court-martial? Indeed, the void-for-vagueness doctrine was meant to prohibit enforcement of offenses with such serious notice deficiencies. Moreover, any assertion that the prosecuting authorities would never charge a Soldier for such minor misconduct cannot cure the constitutional violation. *See United States v. Stevens*, ___ U.S. ___, 130 S.Ct. 1577, 1591 (2010) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.").

53. Therefore, because the Government's interpretation of "exceeds authorized access" renders Section 1030(a)(2)(C) unconstitutionally vague, it cannot be adopted by this Court for any provision of Section 1030. *See Corley*, 556 U.S. at 314; *Powerex Corp.*, 551 U.S. at 232; *Nosal III*, 676 F.3d at 859. Accordingly, sound principles of statutory construction require that this Court adopt the Defense's interpretation of this phrase.

CONCLUSION

54. For the reasons articulated above and in the Defense Motion, the Defense requests this Court

to dismiss Specifications 13 and 14 of Charge II because the Government has failed to allege that PFC Manning's alleged conduct exceeded authorized access.

Respectfully submitted,

DAVID EDWARD COOMBS
Civilian Defense Counsel